REMARKS

Applicant respectfully requests reconsideration of this application. Claims 1-28 are currently pending.

Claims 1, 6, 8, 11, 13, 15, 16, 21, 23, 25, 26, and 28 have been amended. Claims 7, 12, and 22 have been cancelled. No claims have been added.

Therefore, claims 1-6, 7-11, 13-21, and 23-28 are now presented for examination.

Response to Arguments

In response to Examiner's argument with regard to showing nonobviousness, it is submitted the Examiner's statement is incorrect because the Final Office Action has misinterpreted the cited decisions. Following the logic of the Final Office Action in this case, it would be impossible for any Applicant to prove nonobviousness because any discussion of the individual references would be "attacking the references individually". This is a logical and legal absurdity. Each reference can and must be discussed on its own – this is not contrary to the Keller and Merck decisions.

The point of the Keller decision is that it is the combined teaching of the references that is relevant. "The test in determining whether a claimed invention would have been obvious is what the combined teachings of the references would have suggested to one of ordinary skill in the art. In re Keller, 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981)." In re Stencel, 828 F.2d 751, 4 U.S.P.Q.2d 1071 (Fed. Cir. 1987) The Examiner has cited the references as teaching certain claim elements, and the Applicant has shown that the references do not contain these teachings. If the references are examined and it can shown that none of the references teaches or suggests the

relevant claim elements, then it must follow that the combined teaching of the references lacks these claim elements as well, and the claims are not obvious.

Claim Rejection under 35 U.S.C. §103

Trusted Platform Module White Paper

The Examiner rejected claims 1-28 under 35 U.S.C. §103(a) as being unpatentable over Trusted Platform Module White Paper ("*TPM*") in view of Applied Cryptography ("*Applied Cryptography*") and TCG Main Specification Version 1.1a ("*TCG*").

Claim 1, as amended here, is as follows:

1. A method comprising:
   requesting a service for a platform from a service provider;
   receiving a service key request for the service from the service provider, wherein the service key is to be restricted to one or more acceptable configurations of the platform, the configuration of the platform being represented by a set of platform configuration registers, the service provider having a policy regarding which configurations are acceptable, the acceptable configurations being represented by allowable combinations of values of the platform configuration registers;
   generating a service key pair that is restricted to the platform configuration register values for the one or more acceptable configurations of the platform, the service key pair including a public key and a private key, and returning the public key of the key pair to the service provider;
   certifying the use of the service for the one or more acceptable configurations of the platform; and

receiving a session key for a session of the service from the service provider, the session key being bound with the public key of the service key pair, wherein the private key of the service key pair may be utilized to unbind the session key only if the configuration of the platform matches the one or more acceptable configurations to which the service key is restricted.

The claim thus includes "receiving a service key request for the service from the service provider, wherein the service key is to be restricted to one or more acceptable configurations of the platform", "the configuration of the platform being represented by a set of platform configuration registers, the service provider having a policy regarding which configurations are acceptable, the acceptable configurations being represented by allowable combinations of values of the platform configuration registers", "generating a service key pair that is restricted to the platform configuration register values for the one or more acceptable configurations of the platform", "certifying the use of the service for the one or more acceptable configurations of the platform" and "the session key being bound with the public key of the service key pair, wherein the private key of the service key pair may be utilized to unbind the session key only if the configuration of the platform matches the one or more acceptable configurations to which the service key is restricted". It is respectfully submitted that the cited references do not teach or reasonably suggest these claim limitations.

The Office Action indicates that *TPM* "does not disclose the public key (service key) being bound to one or more configurations of the platform or exchanging a session key." This again does not precisely follow the language of the claim, but, as the claims

are now amended, Applicant understands this to mean that *TPM* thus does not provide for "receiving a service key request for the service from the service provider, wherein the service key is to be restricted to one or more acceptable configurations of the platform", "generating a service key pair that is restricted to the platform configuration values of the one or more acceptable configurations of the platform", "certifying the use of the service for the one or more acceptable configurations of the platform" and "the session key being bound with the public key of the service key pair, wherein the private key of the service key pair may be utilized to unbind the session key only if the configuration of the platform matches the one or more acceptable configurations to which the service key is restricted". (Claim 1) (Emphasis added)

In addition to the other differences between claim 1 and the cited reference that have been described in previous responses, the *TPM* reference does contain any discussion regarding platform configuration registers, or the restriction of a key to values of the platform configuration registers. Further, there is no teach or suggestion in the cited reference with regard to the session key being bound with the public key of the service key pair where the private key of the service key pair may be utilized to unbind the session key only if the configuration of the platform matches the one or more acceptable configurations to which the service key is restricted. This further demonstrates that the cited reference does not teach or suggest the elements of claim 1.

The Final Office Action again indicates that *TCG* discloses a command (TPM_Seal) "that stores a secret key to a configuration of the platform configuration registers." It is again respectfully submitted that the suggested operation is not relevant to the claim elements at issue. The TPM_Seal operation is one of a number of processes

by which a TPM protects confidential data. "This section introduces the processes by which a TPM may act as the portal to confidential data stored on arbitrary storage media." (*TCG*, §7, p. 145) This thus is not related to the provision of services, but rather to the unlocking of secrets. As a part of the protection of secrets, the TPM_Seal command allows for the concatenation of additional information to "seal" the confidential data. As described in the specification, the Bind command and the Seal command are described as follows:

> TSS_Bind: External data is encrypted under a parent key. (TPM_UnBind decrypts the blob using the parent key and exports the data from the TPM.)
>
> TPM_Seal: External data is concatenated with a value of integrity metric sequence and encrypted under a parent key. (TPM_Unseal decrypts the blob using the parent key and exports the plaintext data if the current integrity metric sequence inside the TPM matches the value of integrity metric sequence inside the blob). The sealer of the data may specify that no integrity metrics are required.

(*TCG*, §7, p. 146) Thus, in general the difference between the binding operation and the sealing operation is that in the latter case the external data is concatenated with "a value of integrity metric sequence".

This is further explained in section 7.2.1 of *TCG*, which describes the command in detail and indicates that:

> The SEAL operation allows software to explicitly state the future "trusted" configuration that the platform must be in for the secret to be revealed. The SEAL operation also implicitly includes the relevant platform configuration (PCR-values) when the SEAL operation was

performed. The SEAL operation uses the tpmProof value to BIND the blob to an individual TPM.

(*TCG*, §7.2.1, p. 151) Thus, in this operation, there is an additional assurance that a particular "trusted configuration" is present in order for a secret to be revealed. The reason this is done is to provide assurance of the platform that is seeking the confidential data:

> For example, if SEAL is used to store a secret key for a future configuration (probably to prove that the platform is a particular platform that is in a particular configuration), the only requirement is that that key can be used only when the platform is in that future configuration. Then there is no interest in the platform configuration when the secret key was SEALed. An example of this case is when SEAL is used to store a network authentication key.

(*TCG*, §7.2.1, p. 151) Thus, seal does provide additional identify information that is tied to the configuration of the platform when the confidential information is requested.

As was indicated in the last response, in order to analogize the cited reference to the claims here (ignoring other differences between the claims and the references), the command in the *TCG* reference only limits who can get the confidential information – it does nothing to limit where the information is used. Once the confidential information is available, the reference does not address the use of the data, or, in particular, the configuration of the platform in which the data might be used.

The claim limitations that are at issue are not directed to simply obtaining confidential data, as are the cited portions of the *TCG* reference, but rather to generating a service key pair that is restricted to the one or more acceptable configurations of the

platform, certifying the use of the service for the one or more acceptable configurations of the platform, and providing service that is limited to the one or more acceptable configurations of the platform.

Thus, it is submitted that the cited portion of *TCG* is not relevant to service keys that are limited to one or more configurations because the claims regard limiting operations to the one or more configurations, something that the TPM_Seal does not do and does not contemplate – the use of services is not discussed in the reference. The limitations provided in claim 1 are not shown in this reference.

The Office Action also again cites to *Applied Cryptography* as disclosing "a hybrid cryptosystem that is used to exchange a session key by using public key cryptography." This concept does appear to be discussed in this reference, but again this is only relevant to limiting the access to the session key, which again is a question of protecting confidential data and ensuring only authorized persons obtain such data. This does not address the restriction on the use of the session key – the session key would apparently be usable under any configuration of a platform.

Thus, it is submitted that none of the cited references teach or suggest the claim elements of "receiving a service key request for the service from the service provider, wherein the service key is to be restricted to one or more acceptable configurations of the platform", "the configuration of the platform being represented by a set of platform configuration registers, the service provider having a policy regarding which configurations are acceptable, the acceptable configurations being represented by allowable combinations of values of the platform configuration registers", "generating a service key pair that is restricted to the platform configuration register values for the one

or more acceptable configurations of the platform", "certifying the use of the service for the one or more acceptable configurations of the platform", or "the session key being bound with the public key of the service key pair, wherein the private key of the service key pair may be utilized to unbind the session key only if the configuration of the platform matches the one or more acceptable configurations to which the service key is restricted". Thus, because NONE of the references teaches or suggests these claim elements, the references, separately or in combination, do not teach or reasonably suggest all of the elements of claim 1.

It is submitted that the arguments presented above with regard to claim 1 are also applicable to independent claims 8, 13, 16, 23, and 26.

The remaining rejected claims, while having other differences with the cited references, are dependent claims, and are allowable as being dependent on the allowable base claims.

Conclusion

Applicant respectfully submits that the rejections have been overcome by the amendment and remark, and that the claims as amended are now in condition for allowance. Accordingly, Applicant respectfully requests the rejections be withdrawn and the claims as amended be allowed.

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (503) 439-8778 if there remains any issue with allowance of the case.

Request for an Extension of Time

The Applicant respectfully petitions for a one-month extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. §1.136(a). Please charge any fee to our Deposit Account No. 02-2666.

Charge our Deposit Account

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: October 20, 2008

/Mark C. Van Ness/
Mark C. Van Ness
Reg. No. 39,865

1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(503) 439-8778